



■■ Scams, Traps & Your Rights — Complete Guide

10 ways UK consumers are losing money right now — the 5 scams to spot and the 5 legal traps to fight back against. Includes the exact wording and legal rights you need to protect yourself.

■ **The Numbers:** Nearly £1 billion lost to scams by UK consumers in 2025. Almost half of UK adults targeted. Investment fraud alone accounted for 47% of all scam losses by value. And that doesn't count the billions lost to legal traps — hidden fees, fake urgency, impossible-to-cancel subscriptions — that companies have been allowed to get away with for years. Until now.

PART 1 — The 5 Scams Targeting UK People Right Now

These are not unsophisticated operations. They are well-funded, professionally designed, and updated constantly to stay ahead of public awareness. If you have been caught by one — it is not a reflection of your intelligence. It is a reflection of how sophisticated these attacks have become.

■ SCAM 1 — INVESTMENT AND CRYPTO SCAMS

How it works:

You see an advert — often on social media — for an investment platform offering exceptional returns. Sometimes it features a celebrity endorsement that is AI-generated or completely fabricated. You invest a small amount. The platform shows 'returns' growing. You invest more. When you try to withdraw — you can't. The platform eventually disappears.

Warning signs:

- Guaranteed returns — no legitimate investment guarantees returns.
- Pressure to act fast — 'this opportunity closes tonight.'
- Contact only via WhatsApp or Telegram.
- Platform not listed on the FCA Register.
- Anyone asking you to move money to a 'safer wallet' or 'recovery account.'

What to do:

- ✓ Check every investment platform on the FCA Register BEFORE investing: fca.org.uk/register
- ✓ If not on the register — do not invest. Walk away. Always.
- ✓ Never invest based on a social media advert alone — always verify independently.
- ✓ If you've been caught: report to Action Fraud (actionfraud.police.uk) and your bank immediately.
- ✓ Ask your bank about APP fraud reimbursement — mandatory from October 2024.



■ SCAM 2 — AI VOICE CLONING AND DEEPFAKE IMPERSONATION

How it works:

Using audio as short as a brief clip from social media, scammers can clone a voice — your child, parent, or partner. You receive a call that sounds exactly like them. They are in distress. They need money urgently. Don't tell anyone. Transfer now. Also used to impersonate bank staff, police, and HMRC.

Warning signs:

- A call from a family member asking for urgent money transfer.
- Pressure not to tell anyone else or hang up.
- The caller cannot answer personal questions only your family would know.
- Request to transfer money rather than use any other solution.
- Any call from 'your bank' asking you to move money to a 'safe account.'

What to do:

- ✓ Agree a family safe word NOW — before you ever need it.
- ✓ If someone calls claiming to be a family member and cannot give the safe word — hang up.
- ✓ Your bank will NEVER ask you to move money to a safe account. Ever.
- ✓ Call back on a number you know is real before taking any action.
- ✓ Report AI-assisted fraud to Action Fraud: 0300 123 2040.



■ SCAM 3 — SIM SWAP FRAUD

How it works:

Scammers gather your personal details — from a data breach, phishing, or social media. They contact your mobile network pretending to be you, claim your phone is lost, and ask to transfer your number to a new SIM they control. Your phone goes dead. Within minutes they use your number to reset passwords and access bank accounts. SIM swap fraud rose 38% in 2025.

Warning signs:

- Unexpected loss of mobile signal for no obvious reason.
- Text messages or emails about a SIM transfer you did not request.
- Inability to make calls or access mobile data.
- Notifications of password resets you did not initiate.

What to do:

- ✓ Call your mobile network NOW and add a verbal password to your account.
- ✓ Remove SMS as your two-factor authentication method — use an authenticator app instead.
- ✓ If you lose signal unexpectedly — call your network IMMEDIATELY from another device.
- ✓ Freeze your bank accounts if you suspect a SIM swap has occurred.
- ✓ Report to Action Fraud and your mobile network.



■ SCAM 4 — FAKE GOVERNMENT AND FINE WEBSITES

How it works:

You receive a text or email appearing to be from HMRC, the DVLA, Royal Mail, or a parking authority. It claims you owe a penalty and must pay immediately. The linked website looks completely legitimate — correct logos, official-looking design, almost-correct URL. Your card details are stolen the moment you enter them. Some sites also install malware on your device.

Warning signs:

- HMRC, DVLA, or Royal Mail contacting you by text demanding urgent payment.
- A link to a website — always check the URL character by character.
- Threats of immediate legal action or bailiffs.
- A request to pay a small fee to release a parcel.

What to do:

- ✓ HMRC does not text you to demand payment. DVLA does not text about fines. Royal Mail leaves a card.
- ✓ Never click a link in an unsolicited text or email — go directly to gov.uk in your browser.
- ✓ Forward suspicious texts to 7726 (free — works on all major networks).
- ✓ Forward suspicious emails to report@phishing.gov.uk
- ✓ If you have already entered card details — contact your bank immediately to cancel the card.

■ SCAM 5 — GHOST SUBSCRIPTIONS AND PURCHASE SCAMS

How it works:

You buy something from a social media advert. It never arrives — or it is nothing like the description. Separately, recurring charges appear on your bank statement for services you either never signed up to, or signed up to once and forgot. These are often small amounts — £2.99, £4.99 — specifically designed to avoid triggering your attention.

Warning signs:

- Small unfamiliar recurring charges on bank statements.
- Social media adverts for products at unrealistically low prices.
- Reviews that appear too good, too numerous, or too recent.
- No easily findable company address, phone number, or returns policy.

What to do:

- ✓ Review your bank statement RIGHT NOW for any recurring charge you cannot identify.
- ✓ Call your bank and request cancellation of any unrecognised recurring payment.
- ✓ Before buying from any social media ad — search the company name plus 'reviews' independently.
- ✓ If you paid on a credit card and goods never arrived — make a Section 75 claim (see Part 2).
- ✓ If paid by debit card — request a chargeback from your bank within 120 days.



PART 2 — The 5 Legal Traps Companies Use Against You

These are not mistakes. Every one of these practices was deliberately designed to cost you money while keeping it technically legal. Several have recently become illegal. Here is what changed and what you can now do about it.

■ TRAP 1 — DRIP PRICING

What it is:

You see a price. You click through. By checkout you are paying significantly more — admin fees, booking fees, digital access charges, compulsory insurance — all added incrementally as you proceed. The CMA found drip pricing in 93% of event ticket sites, 69% of cinema sites, and 60% of gyms reviewed. The AA was fined £4.2 million for it in April 2026.

The law:

Drip pricing is now illegal under the Digital Markets, Competition and Consumers Act 2024 (DMCC Act), which came into force in April 2025. Businesses must show the total price — including all mandatory fees and charges — at the point of invitation to purchase, not at checkout.

What to do:

- ✓ If you paid more than the advertised headline price due to hidden fees added at checkout — you have grounds to complain.
- ✓ Write to the company citing the DMCC Act 2024 and request a refund of the undisclosed charges.
- ✓ If they do not respond — escalate to the Competition and Markets Authority (gov.uk/cma) or relevant ombudsman.
- ✓ Check whether you paid by credit card — Section 75 may also apply.



■ TRAP 2 — FAKE REVIEWS

What it is:

Product and service reviews are the primary decision-making tool for most online purchases. Fake reviews — paid-for five-star ratings, suppressed negative reviews, review manipulation — are widespread across online marketplaces, restaurant platforms, and retail sites. The CMA issued advisory letters to over 50 companies in 2025 about non-compliance.

The law:

Fake reviews are now banned under the DMCC Act 2024. Online marketplaces must take reasonable and proportionate steps to ensure reviews on their platforms are genuine. Commissioning fake reviews is now a specific automatically-unlawful practice.

What to do:

- ✓ Before purchasing, look for review patterns — a sudden flood of 5-star reviews in the same week is suspicious.
- ✓ Use Fakespot (fakespot.com) or ReviewMeta (reviewmeta.com) to check review authenticity.
- ✓ If you bought a product based on reviews that turn out to be demonstrably fake — you may have a misrepresentation claim.
- ✓ Report suspected fake reviews to the CMA: gov.uk/cma



■ TRAP 3 — SUBSCRIPTION DARK PATTERNS

What it is:

Companies make signing up instant and cancellation deliberately difficult — burying the cancel button, requiring phone calls during limited hours, deploying 'retention specialists' trained to prevent you leaving, or quietly rolling free trials into paid subscriptions without adequate notice.

The law:

Current law (Consumer Contracts Regulations 2013): you have a statutory 14-day right to cancel any subscription signed up to online, and companies must make cancellation reasonably accessible. Most companies ignore both obligations. New rules under the DMCC Act — expected to come into force in spring 2027 — will go significantly further: requiring reminder notices before trials convert, cancellation as easy as sign-up, and renewal cooling-off periods. Those rules are not yet in force. The 14-day right and the reasonableness obligation are.

What to do:

- ✓ If you signed up within the last 14 days — invoke your statutory right to cancel under the Consumer Contracts Regulations 2013.
- ✓ If the company never told you about your cancellation rights at sign-up, your window may be up to 12 months and 14 days.
- ✓ Write to the company asserting your statutory right. Do not accept 'company policy' as a reason to refuse.
- ✓ If you paid by credit card — ask your bank to stop future payments immediately.
- ✓ If the company continues to charge after cancellation — raise a formal complaint and escalate to the Financial Ombudsman.
- ✓ Report persistent dark patterns to the CMA: gov.uk/cma



■ TRAP 4 — SECTION 75 — THE LEGAL WEAPON MOST PEOPLE NEVER USE

What it is:

This is not a trap companies set — it is a trap most consumers fall into by not knowing this right exists. Section 75 of the Consumer Credit Act 1974 makes your credit card company jointly and equally liable with the seller for any breach of contract or misrepresentation. It applies to purchases between £100 and £30,000 on a credit card — and even if you only paid a deposit on the card, you can claim the full amount.

The law:

Section 75 of the Consumer Credit Act 1974. Your credit card company is jointly and severally liable with the seller. This is a statutory right — not a company policy. It cannot be refused on the grounds that the seller is now insolvent or uncontactable. Debit cards are not covered (use chargeback instead).

What to do:

- ✓ Contact your credit card company and state clearly: 'I am making a claim under Section 75 of the Consumer Credit Act 1974.'
- ✓ Provide: what you bought, when, how much you paid, what went wrong, and evidence of attempts to resolve with the seller.
- ✓ If the seller has gone bust — go straight to your credit card company. You do not need to pursue the seller first.
- ✓ If your credit card company rejects the claim — escalate to the Financial Ombudsman Service (free): financial-ombudsman.org.uk
- ✓ You have up to 6 years from the date of the breach to bring a court claim. Note: the Financial Ombudsman Service typically requires complaints within 6 years of the problem, or 3 years from when you became aware of it — whichever is later. Do not delay.



■ TRAP 5 — THE 14-DAY COOLING-OFF PERIOD

What it is:

You have a statutory right to cancel almost any purchase made online, by phone, or at the door within 14 days — no reason needed. Many companies deliberately obscure this right, making the process confusing enough that the window passes before you have figured out how to use it. Exceptions include perishable goods, made-to-order items, and digital content already downloaded.

The law:

Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013. This is a statutory right — not a company policy. Critical: if the company never told you about this right at the point of purchase, the window extends to 12 months and 14 days.

What to do:

- ✓ For any online, phone, or doorstep purchase — the 14-day cancellation window starts from the day you receive the goods.
- ✓ State clearly in your cancellation: 'I am exercising my statutory right to cancel under the Consumer Contracts Regulations 2013.'
- ✓ If the company never provided information about your cancellation rights — your window may be 12 months and 14 days.
- ✓ Cancel in writing and keep a copy. Email is sufficient.
- ✓ If the company refuses to honour the cancellation — escalate to the Financial Ombudsman or Citizens Advice.

PART 3 — Quick Reference and Key Contacts

1. The Exact Words to Use

Situation	Say or write these exact words
Section 75 claim	'I am making a claim under Section 75 of the Consumer Credit Act 1974.'
14-day cancellation	'I am exercising my statutory right to cancel under the Consumer Contracts Regulations 2013.'
Drip pricing complaint	'I am complaining under the Digital Markets, Competition and Consumers Act 2024 regarding undisclosed fees.'
Subscription cancellation	'I require you to cancel my subscription immediately and confirm in writing.'
Refusing police phone search	'I do not consent to my phone being searched without a warrant.'

2. Where to Report Each Type

What happened	Where to report
---------------	-----------------



Financial scam / investment fraud	Action Fraud: actionfraud.police.uk / 0300 123 2040. Also FCA: fca.org.uk/consumers/report-scam
Phishing text or email	Texts: forward to 7726 (free). Emails: report@phishing.gov.uk
Drip pricing / fake reviews	Competition and Markets Authority: gov.uk/cma or Citizens Advice: citizensadvice.org.uk
Credit card dispute / Section 75	Your credit card company first. Then Financial Ombudsman: financial-ombudsman.org.uk
Subscription / cancellation dispute	Financial Ombudsman (financial services). Citizens Advice for others.
Fake investment not on FCA register	FCA ScamSmart: fca.org.uk/scamsmart

3. Your 10-Point Protection Checklist

- Check every investment platform on the FCA Register before investing: fca.org.uk/register
- Agree a family safe word for emergency phone calls — before you need it.
- Add a verbal password to your mobile account to prevent SIM swap fraud.
- Replace SMS two-factor authentication with an authenticator app.
- Review your bank statement monthly for unrecognised recurring charges.
- Never click links in unsolicited texts or emails — type the address directly into your browser.
- Pay for significant purchases over £100 on a credit card — not a debit card — to preserve Section 75 rights.
- Know your 14-day cancellation right exists and how to invoke it before you need it.
- Always search a company's name plus 'reviews' or 'scam' independently before buying from an ad.
- Keep copies of all purchase confirmations, correspondence, and receipts.

4. Key Terms Explained

Term	Plain English
APP Fraud	Authorised Push Payment fraud — you are tricked into authorising a payment yourself. Now subject to mandatory bank reimbursement rules.
Section 75	A provision of the Consumer Credit Act 1974 making your credit card company jointly liable for failed purchases between £100 and £30,000.
Chargeback	A voluntary scheme allowing debit card providers to reverse a transaction. Not a legal right like Section 75, but useful for smaller amounts or debit card purchases.
Drip Pricing	The practice of showing a low headline price and adding mandatory fees incrementally at checkout. Now illegal under the DMCC Act 2024.
Dark Patterns	Deliberate design choices that manipulate users — confusing cancellation flows, pre-selected add-ons, fake countdown timers. Increasingly illegal.



SIM Swap	Fraud where criminals transfer your mobile number to a SIM they control, allowing them to intercept one-time passcodes and access your accounts.
DMCC Act 2024	Digital Markets, Competition and Consumers Act. The major new consumer protection law that came into force in April 2025, banning drip pricing and fake reviews.

5. Key Contacts and Resources

- **Action Fraud:** actionfraud.police.uk / 0300 123 2040
- **FCA ScamSmart:** fca.org.uk/scamsmart
- **FCA Register (check investment firms):** fca.org.uk/register
- **Report phishing texts:** Forward to 7726 (free)
- **Report phishing emails:** report@phishing.gov.uk
- **Financial Ombudsman:** financial-ombudsman.org.uk / 0800 023 4567
- **Competition and Markets Authority:** gov.uk/cma
- **Citizens Advice:** citizensadvice.org.uk / 0800 144 8848
- **Better Call Kal — templates and referrals:** bettercallkal.co.uk

Disclaimer

*This guide is for **general education only**. It is **not legal or financial advice**. Laws change — always verify current rules. If you have been a victim of fraud, contact your bank and Action Fraud immediately.*

© Better Call Kal 2025. All rights reserved.